

WHAT IS CLAIMED IS:

1. A method for protecting electronic content from unauthorized use, the method including:

receiving a request to access a piece of electronic content;

identifying one or more software modules responsible for processing the piece of electronic content;

evaluating one or more predefined characteristics of the one or more software modules;

denying the request to access the piece of electronic content if the one or more predefined characteristics fail to satisfy a set of predefined criteria.

2. A method as in claim 1, further including:

using the predefined criteria to evaluate a predefined policy, and basing a decision to deny the request on the outcome of this evaluation.

3. A method as in claim 1, in which evaluating one or more predefined characteristics of the one or more software modules includes computing the cryptographic hash of at least one of the one or more software modules.

4. A system for protecting electronic content, the system comprising:

means for applying a cryptographic fingerprint to the electronic content;

means for evaluating one or more predefined characteristics of the drivers responsible for handling the electronic content;

means for denying effective access to the electronic content based on an output of said means for evaluating one or more predefined characteristics of the drivers responsible for handling the electronic content;

20

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

means for generating an identifier associated with the electronic content;

means for monitoring a predefined system interface for data containing the identifier;

means for preventing effective access to data containing the identifier via the predefined system interface.

- 5.
- A method for protecting electronic content from unauthorized use, the method including:

(a) receiving a request to access a piece of electronic content;

(b) generating a first identifier associated with the electronic content;

(c) monitoring at least one system interface, the monitoring including:

(1) receiving a piece of electronic data;

(2) generating a second identifier associated with the piece of electronic data;

(3) comparing the second identifier with the first identifier;

(4) taking a predefined defensive action if the second identifier is related to the first identifier in a predefined manner.

- 6.
- A method as in claim 5, further including:

(a)(1) decrypting the electronic content.

- 7.
- A method as in claim 5, in which the first identifier comprises a hash of at least a portion of the electronic content, and in which the second identifier comprises a hash of at least a portion of the piece of electronic data.

- 8.
- A method as in claim 5, in which the first identifier comprises a predefined portion of the electronic content and in which the second identifier comprises a predefined portion of the piece of electronic data.

- 5
- 10
- 15
- 20
9. A method as in claim 5, in which the system interface comprises a file system interface to one or more device drivers.
 10. A method as in claim 5, in which the predefined defensive action comprises modifying at least a portion of the piece of electronic data.
 11. A method as in claim 10, in which modifying at least a portion of the piece of electronic data includes scrambling at least a portion of the piece of electronic data.
 12. A method as in claim 5, in which the predefined defensive action comprises adding noise to at least a portion of the piece of electronic data.
 13. A method as in claim 5, in which the predefined defensive action comprises adding an electronic watermark or fingerprint to at least a portion of the piece of electronic data.
 14. A method as in claim 5, in which the predefined defensive action comprises preventing the transfer of at least a portion of the piece of electronic data to an output device via the system interface.
 15. A method as in claim 5, in which the predefined relation between the first identifier and the second identifier comprises the first identifier being equal to the second identifier.
 16. A method as in claim 5, in which the at least one system interface is selected using rules associated with the electronic content, the rules being operable to identify certain system interfaces to which the electronic content is not allowed to be sent.
 17. A method as in claim 9, in which the one or more device drivers are selected from the group consisting of: video display driver, sound driver, SCSI driver, IDE driver, network driver, video capture driver, floppy disk driver, and scanner driver.
 18. A method as in claim 5, further comprising:

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L. L. P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6800

